TITLE: As it more accurately describes the invention, Applicant amends the title from "Method for Certifying and Unifying Delivery of Electronic Packages" to PROOF OF SERVICE – ELECTRONIC (PoS-e). A corresponding replacement sheet 1 with the later title is attached.

History

This patent application began as a PCT filing. It subsequently entered the national phase, including filing with the USPTO. Applicant has *pro se* filed in various countries, including Canada, Australia, and New Zealand and through counsel in the EU.

A PCT Written Opinion under PCT Rule 66 was issued on 10 Feb 2003 disallowing claims 1-14 and 16-22 and allowing claim 15.

Applicant's response was filed timely arguing, *inter alia*, that prior art relied upon to disallow claims 1-14 and 16-22 was a misunderstood reference, that PoS-e presented a new principle of operation and solved a different problem; further, Applicant added claims 23-82. Applicant also modified certain Figures and clarified the term "In Camera Key" indicating that "in camera" means "secret".

Reply to the First Office Action

A PCT Notification of Transmittal of International Preliminary Examination Report was issued on 2 Jul 2003 stating that "Claims 1-13, 15-82 meet the criteria set out in PCT Article 33(2)-(4) because the prior art does not teach or fairly suggest the creation of an electronic certificate of service as an encrypted file in encrypted PDF form that is therefore printable, but can't be modified."

The PCT also stated, "Claims 1-13, 15-82 meet industrial applicability as defined by PCT Article 33(4). The use of a unitary system for the certifiable delivery of electronic packages is useful for secured internet commerce."

Following as Exhibit "A" is a complete copy of the PCT Notification issued 2 Jul 2003, the contents of which are incorporated herein by this reference as though set forth in full as a similar amendment for the purposes of this Office Action. Request is hereby made that the United States Patent & Trademark Office take Official Notice of the Allowances made by PCT.

Request of Inventor

Inventor was surprised to learn that his counsel did not supply to the Examiner Exhibit "A" (the results of the PCT acceptance of claims 1-13 and 15-82) and has undertaken to finish this application *pro se*.

Inventor respectfully requests that the Examiner assist in the drafting of one, or more, claims for Applicant. In light of the acceptance by PCT, it is clear that PoS-e presents a patentable, commercially useful and generally helpful invention worthy of the effort.

Additionally, Applicant has amended the specification and claims of this application so that they are proper, definite, and define novel structures which are also unobvious. If, for any reason the application is not now believed to be in full condition for allowance, Applicant respectfully requests the constructive assistance and suggestions of the Examiner pursuant to M.P.E.P. § 2173.02 and § 707.07(j) in order that the undersigned can place this application in allowable condition as soon as possible and without the need for further proceedings.

Purpose of the Invention:

Proof of Service – electronic was intended to solve a duality of issues:

First: Everyone desires that their communications over the internet be performed securely. PoS-e accomplishes this by utilizing SSL encryption for transferring of files and messages. No claim is made for these features because clearly such is in the public realm;

Second: However, at the same time there is the need for an "open" system that can be relied open by the sender and recipients, and interested third parties (called "Entitled Persons" at ¶ 0024) such as a court, escrow, creditor, etc.). PoS-e satisfies this condition utilizing a unique and nonobvious system.

PoS-e satisfies both conditions splendidly as described herein.

Response to Claim Rejections – 35 U.S.C. §102

The Examiner rejected claims 1-4, 7-12, 14, and 16-22 under 35 U.S.C 102(b) as being anticipated by Mitty. In order to make the novelty of the present invention clearer, the claims have been amended to distinguish it from Mitty even though Applicant believes that Mitty is a very different concept.

Overview

Facially Mitty and Proof of Service – electronic (PoS-e) appear similar; however the two systems differ radically, as does their underlying purpose. While Mitty is replete with operational uncertainties, PoS-e is uniquely suited to provide a perfect, stable and transparent solution to the issue of proving service.

Mitty attempts to establish a secret email system. See Col 2, Lines 1-5[1] which states:

> There is a need in the art for an electronic message system that provides privacy, authentication of participants, and non-repudiation. There is, moreover, a particular need for an electronic message system in which it is difficult to detect. (Col 2, Lines 1-5)

Mitty thereafter in its patent proceeds to spell out in great detail how the object of secrecy is to be obtained through the use of third-part, time-limited public key[2] encryption.

PoS-e establishes an open system to prove the delivery of a novel and unique "Proof of Service – electronic" digital file verifying the delivery of an Electronic Package (EP) to anyone, as follows:

> Entitled Person: An Entitled Person is either the sender or recipient, or any other person authorized under applicable law, to receive a copy of the Certificate issued by the Responsible Person. (¶ 0024)

---

1 All Col references are to Mitty. All ¶ references are to PoS-e.

2 All references herein to "public key" references in Mitty refer to Col 5, Lines 4-25 as issues by companies to employees, universities to students, townships to residents, and commercial companies such as Thawte or Verisign, etc.

Accordingly, PoS-e's function is to provide delivery system for electronic document to verifiably prove delivery of an EP, even years in the future, without resort to any third party's public key.

PoS-e has been used in federal court to prove service of summons & complaint and by UPS for the provable electronic delivery of documents. There is no proof that Mitty has been used anywhere, probably because of the weaknesses of Mitty explained herein.

Systemic Differences

Mitty claims a method for ensuring the integrity of a message through a three-fold encryption system – encryption by sender, encryption by intermediary, encryption by recipient. **Mitty facilitates encryption by using public keys** of both the sender and the recipient that are issued by third-parties and which are time-limited – a process fraught with imperfection and highly prone to failure for the reasons set forth below.

PoS-e creates a secure and *independent* proof of service through independent encryption and certification by PoS-e's CA function (¶¶ 0020 and 0028). Essentially, PoS-e is a server-side application accessed from the web through standard server-side authentication protocols.

As such there are different roles played by sender, CA, and recipient in the PoS-e system that are distinguishing and novel over the relevant art cited in the Office Action.

Mitty allows the sender to assemble an EP and then transmits the entire EP to the recipient, storing only a summary of the transmission. Again, this is a system fraught with frailty as explained below.

PoS-e requires that the sender access its secure server and then **PoS-e assembles the EP itself** (See PoS-e Figure 7) utilizing inputs from the sender. The PoS-e server uploads the message and attachments (if any) using a SSL connection. (¶ 0126)

Below is an ordered outline of the differences of PoS-e over Mitty relative to the changes made in the amendments to the claims.

Sender Differences:

Package Initiation:

In the Mitty patent, the "Intermediary" indiscriminately receives electronic packages (EP) from a sender.

This is distinguishable and inappropriate for the use of the present invention. In PoS-e, the sender must first log on to a server before an EP can be sent. In this way, only those who are authorized to send EPs may have one created by the CA.

Further, and unlike the Mitty patent, in PoS-e it is the sender that initiates the EP that is later to be certified as delivered by the CA function of PoS-e. In all independent claims for Mitty, the sender transmits an EP as "responsive to a message transmit request from a user." (Mitty claims 1, 3, 6, 11, and 12)

The Claims herein have been restated to make sender initiation clear by requiring the sender to log on to a server in order to have the server create the EP.

Sender Authentication:

In effect, the PoS-e system is a subscription service. (¶ 0056) The Mitty patent is not. Authentication for Mitty is subsumed by the encryption that must execute independently on all three actors – sender, intermediary, and recipient.

As such, there is no authentication requirement that needs to be performed prior to the transmission of an EP. This is not the case with PoS-e, which requires the additional step of "logging on" to a CA that, presumes authentication – whether by traditional methods or other methods of subscription. This is further evidenced by the method of delivery, as also laid out in the Summary of the Invention, which states that PoS-e provides:

> "An exemplary method [including]: (1) Making available to a person who subscribes to the PoS-e service the ability to securely utilize either (a) her email client, or (b) a web-based email system, to assemble an email transmission..."

The requirement of PoS-e to require the sender to log on to a CA in order to send a message is made more apparent by the amendment to Claim 1 requiring this embodiment.

Creation of the Electronic Package:

In Mitty's secure, non-subscription email system, the EP is initially created by the sender who then transmits the completed package to the intermediary.

There is no such requirement for PoS-e. Instead, and in order to conform to a truly independent Certifying Authority (CA), the EP is created by the CA as a response to inputs or elections made by the sender after logging on to the CA. This is critical to maintaining complete integrity and independence by the CA in the overall PoS-e system.

To reflect this key difference, The Claims herein have been restated to show this embodiment.

Sender Encryption:

Separate Encryption Requirement: In Mitty, the encryption method for the sender is executed as a "separate thread on the client". (Col 1, Lines 53-55) This is reflected in the language of the claims requiring the sender to have a "first logic" capable of forming an "encrypted version of the message." (Mitty, Independent claims 1, 3, 11, and 12) This would defeat the purpose of PoS-e of creating a true proof of service by a truly independent CA.

Similarly, multiple encryption is a requirement of the Mitty patent where the sender must twice encrypt the EP on the client-side in order to be decrypted by the trusted intermediary (outer envelope) and the recipient (inner envelope).

Nowhere is this claimed nor disclosed by the PoS-e application because it is unnecessary since PoS-e is a open system while Mitty is a secret system.

In effect, it is not Mitty that is providing authentication but the person sending the message because it is the public key of the sender that Mitty relies upon initially.

With PoS-e, *all encryption is localized to the PoS-e CA function*. This accomplishes what is not found in the prior art which is an "independent person [who] attests to the transmission of specified documents to a specified party." (PoS-e Application, Description of the Related Art, paragraph 0007)

The Claims herein have been restated to reflect the authentication and encryption by the CA and requiring the CA to create a unique identification and hash value for the EP.

Certifying Authority & Trusted Intermediary Differences:

Data Storage:

Because the Mitty patent discloses a secure email system, the "trusted intermediary" of Mitty nowhere claims nor discloses storing data other than data "indicative of the status of a transaction" (Mitty, claims 1, 3, 6, 11, and 12)

Furthermore, the Mitty specification only ever discloses storing the "the status of transactions" including only information relevant to the reception of the message; confirmation of the message; unique identifiers; and other status archives. (Mitty, Detailed Description, Page 11, Column 1, Lines 26-43)

With PoS-e, and in order to comply with governmental guidelines requiring data storage for statutory periods of time, data that includes the actual documents desired to be confirmed as delivered and other attachments are also stored and made available for retrieval for a required amount of time.

Because PoS-e is open, it archives everything, not just filenames.

The Claims herein have been restated to further require the storage of data other than simply the information relating to the transmission of the EP.

In Camera Key:

In the Mitty patent, there are 3 levels of encryption required by each of the sender, intermediary, and recipient. For each of these actors in the Mitty system, there are two levels of encryption and further requirements for decryption. The effect of this system is that each of the actors is enabled to decrypt the EP using their own private key that is inherent in their client-side symmetric encryption process.

The PoS-e system is completely different. PoS-e's "In Camera Key" (ICK)[3] required for decryption is secretly held by the CA and used so it alone can verify PoS-e's embedded Digital Certificate on the "Proof of Service – electronic".

The ICK is a specially encrypted key generated by the CA after confirmation of receipt of the EP at which time there is an immediate and simultaneous delivery to all parties of the PoS-e "Proof of Service – electronic" (¶¶ 0119, 0125, and 0136).

The decryption key is stored on the CA and is *unknown to either the sender or the recipient.* Only until the CA confirms the identity of a requesting party to retrieve the EP will the key be used by PoS-e's CA function, at which time a duplicate EP will be given to them and they will be able to retrieve status

[3] The term "in camera" means "secret".

information and obtain the electronic documents that were the subject of the electronic proof of service.

This is different than what is claimed or disclosed in Mitty where either the sender or the recipient has access to the decryption key for the message being authenticated.

The Claims herein have been restated to reflect the embodiment described above wherein the CA sends to the recipient a message relating to the EP after which, the recipient logs on to the CA to retrieve the message.

Recipient Authentication:

The Mitty patent requires the recipient to verify the contents of incoming packets based on "logic" required to validate receipt of the EP and to decrypt the FP (All independent claims require that the FP be "decryptable by the recipient," Mitty Claim 11)

Conversely, PoS-e requires validation of delivery to the recipient based on the recipient's unique identifier. The recipient does not require special logic or any public key to decrypt data since the unique identifier is either an email address and/or a special "message code or password" created by the CA and

then transmitted to the recipient which is then used as authentication by the recipient in order to log on to the CA to retrieve the EP.

Simply, the recipient never receives the EP formed by the CA as a response to the initiation of the sender until it receives notification by the CA and then logs on to the CA.

Mitty makes reference at Col 13, Lines 59-67 and Col 14, Lines 1-5 to an alternative embodiment permitting a recipient to log on and receive her EP through an HTTP server. However, downloading from an HTTP server utilizes SSL encryption, not public key encryption. There is no known protocol for using public key encryption from three independent parties as required by Mitty for HTTP downloads and there is no specification in Mitty resolving the important issue of "is delivery complete" if the recipient does not, or cannot, decrypt Mitty's download. Thus, Mitty's alternative embodiment will not perform its intended function.

Detailed Responses to Examiner's Rejections:

RESPONSE to 1: There is no Certifying Authority ("CA") in Mitty. The "certification" process described in Mitty is a simple verification over the internet that the sender's and recipient's third-party digital signature is valid. Mitty does not propone or even mention that it acts as a CA.

Mitty does not propone, or even mention, that it issues its own certificate. The issuance of its own certificate is the prime prerequisite to be a CA (15 CFR §2011.102(d)[4], India's "Information Technology Act of 2000" IN 1.5 Certifying Authority[5], United States V. Allen-Bradley Co., 352 U.S. 306, 307[6]).

All Mitty does is facilitate a two-sided verification process of someone else's property (Mitty Col 4, lines 36-59) while protecting the identity of the sender and recipient (Mitty Col 1, lines 36-38). While this may be a valuable function it is clearly nothing akin to PoS-e (See PoS-e ¶0020).

See Mitty at Col 5, lines 4-25 which describes in detail that outside, non-Mitty companies called "certificate authorities" (such as schools, companies, townships, etc.) are relied upon by the Mitty process.

Mitty is not a Certifying Authority! Nowhere in Mitty is a process or method provided whereby Mitty itself certifies anything or issues a self-proving certificate.

---

[4] Certifying authority means a person designated by the government of a foreign country who is authorized to execute and issue certificates of quota eligibility on behalf of such foreign country.
[5] The pre-qualifications for becoming a certifying authority are contained in §21 of the Act. This prescribes that a person applying to become a certifying authority has to fulfill all the criteria relating to qualification, expertise, manpower, financial resources and other infrastructure facilities necessary to the issue of digital signature certificate, as may be prescribed by the government.
[6] "... the War Production Board, which was then the certifying authority, [was asked] for certificates that the improvements were necessary to the national defense. The Board issued nine different certificates..."

Mitty utilizes only its public key/private key encryption process to protect the transmissions flowing through it. For example, Mitty says, "In either case, the logic proceeds to step **455** in which an enveloped Data structure, referred to as M14, is created from M11. MI1 is encrypted using RC2 encryption and a 128 bit key. The key is then encrypted with the public key of intermediary [i.e., Mitty]." (See Col 13 lines 45-56).

PoS-e is a Certifying Authority because it issues its own Digital Certificate (DC) as embodied in its "Proof of Service – electronic" (PoS-e Figure 12) and provides for a specific authority within PoS-e to provide Certification of its own signature (PoS-e ¶ 0020).

RESPONSE TO 1a: Mitty does not in any way act in "receiving an electronic package" except as a mere conduit. Mitty only passes it along because nowhere in Mitty, or in its claims, does it claim to do anything more than save such things as messages, notarizations by third parties and filenames.

An "electronic package" ("EP") consists of a message and the complete attached files (PoS-e ¶ 0025).

Mitty mentions "file" in various places as follows:

Col 7, lines 35-45:

A suitably-equipped personal computer could include hardware security mechanisms, such as hardware tokens, for the storing and processing of private keys, or it could maintain private keys using software techniques. It would also include software for constructing the message that is desired 40 to be sent. This software might include conventional e-mail software that can construct a message with its own editor, or it could include word processing applications, which can construct files that could be included as attachments to an e-mail message.

NOTE: This reference to attachment is of a garden variety PC's capability and not a part of Mitty; therefore no claim can be made for Mitty upon it.

Col 7, lines 55-65:

The logic starts in step **200** and proceeds to step **205.** In step **205** the message to be securely transmitted is gathered along with other information. The message may be of any content type, but an easy-to-understand example would be a text message. The other information gathered includes a 60 copy of a DC for the sender **105** and the recipient(s) **120,** a subject of the message, an account code, filenames, if any, to be attached, and information identifying the desired service levels and options to be performed, e.g., local archiving, electronic notarizing, etc.

NOTE: Only filenames of attachments are collected by Mitty. Thus such is not a party of Mitty and no claim can be made for Mitty upon the collection of filenames.

Col 7, lines 66-67 & Col 8 lines 1-5:

The logic proceeds to step **210** in which an electronic waybill data structure is created and initialized. An exemplary waybill structure includes a local date/time stamp including a time zone, the subject text, the filenames of any attachments, the e-mail address and DC of sender **105,** addresses and certificates for the recipient(s) **120,** an account code, and client's billing code.

NOTE: Only filenames of attachments are collected by Mitty. Thus such is not a party of Mitty and no claim can be made for Mitty upon the collection of filenames.

Col 8, lines 6-9:

The logic proceeds to step **215** in which the file structures of any attachments, the recipient's e-mail address, and the certificates for any recipient(s) and for the intermediary **115** are validated. Conventional techniques are used to validate the file structures and e-mail addresses.

NOTE: "Conventional techniques" are used to validate file structures. Accordingly no claim to validating file structure can be a part of the Mitty patent or in behalf of Mitty.

Col 8, lines 14-17:

The logic proceeds to step **220** in which a multipart/mixed MIME body part, referred to as MI, is created. M1 is created using conventional techniques to combine the message, the attachments, and the subject value gathered in step **205.**

NOTE: "Conventional techniques" are used to combine the message and attachments. Accordingly no claim to combining file structure can be a part of the Mitty patent or in behalf of Mitty.

Col 9, lines 6-12:

For example, using conventional techniques, sender **105** may archive the ID, the digest of the message M1 the digest algorithm identifier, e-mail addresses and certificates for the recipient(s) **120,** subject text, filenames, message length, and various information specific to the services requested, e.g., insurance level, notary information, etc.

NOTE: "Conventional techniques" are used to archive the filename(s). Additionally, only filenames of attachments are archived, not the attached files themselves. Accordingly no claim to validating file structure can be a part of the Mitty patent or in behalf of Mitty.

Col 11, lines 50-55:

More particularly, the new waybill includes the waybill ID, the sequence numbers, the relevant e-mail addresses, message length of MI, subject text, message origination time stamp, filenames of attachments, and service and option related information.

NOTE: Only filenames are included in the waybill. No effort is made to archive the files sent as attachments. Thus no claim can be made by Mitty, or in behalf of Mitty, that attached files are archived.

Col 13, lines 22-27:

This information includes the ID, the sequence number, the relevant e-mail addresses and certificates, service-related information, such as the insurance level, the filenames of any attachments, the length of MI, and time stamp information.

NOTE: Only filenames are included in the waybill. No effort is made to archive the files sent as attachments. Thus no claim can be made by Mitty, or in behalf of Mitty, that attached files are archived.

Col 15, lines 62-64:

The waybill includes status information, indicating whether the authorization passed or failed, among other things, and the inner envelope contains the search results from the VR as an attachment.

NOTE: Here the word "attachment" is mentioned but refers to a file generated by the Mitty process itself.

Accordingly, Mitty cannot be a CA since it does not issue a certification or obligate itself to store a complete copy of all files, which is the essence of a CA's function and without that essence a CA does not exist (See 47USC254(h)(5)((A)(i) and (D) and 19CFR115.12).

PoS-e creates an EP (consisting of a message and attachments) and retains the complete EP for up to ten years (See PoS-e Figure 7). It thereafter acts as a CA to prove up to any Entitled Person ("EP) (See PoS-e ¶ 0024) both the message and the attachments.

Mitty uses third-party public keys which anyone can do – there is no magic to this. The use of a third-party public key does not a Certifying Authority make! Mitty at Col 4, lines 47-49 says "First, the recipient decrypts the digital signature with the sender's public key to recover the digest of the message." This function is simply the usual decryption involved with a digital signature from, say, Thawte or Verisign.

Mitty further advises at Col 4, lines 59-61, "Notice that in the above description, signatures do not provide privacy; the message is never encrypted. Other mechanisms must be used for privacy." Mitty utilizes those other mechanisms to secure privacy as described throughout it patent.

In fact, in its preamble, Mitty states:

> There is a need in the art for an electronic message system that provides privacy, authentication of participants, and non-repudiation. There is, moreover, a particular need for an electronic message system in which it is difficult to detect that a given sender is sending a message to a given recipient.

PoS-e, on the other hand, is a *public* Certifying Authority. The purpose of PoS-e is to provide proof of service of any EP to the Sender, Recipient, a Court, Insurance Company, Regulatory Agency, or any other entity designated. PoS-e is thus exactly the opposite of Mitty in this regard. The purpose for PoS-e is to *prove service* in any of the various settings that service must be proven.

While PoS-e can provide for encryption portal-to-portal (as can any service with an SSL certificate, including encrypting the EP while in storage) – encryption and secrecy are not what PoS-e is all about. For example, see PoS-e at ¶

0056(6) which states that PoS-e will "Mak[e] available to sender the option to encrypt the message and the attachment(s) utilizing strong encryption;..."

RESPONSE TO 1.b: Mitty is not a "Certifying Authority". Nowhere in Mitty is the term even used.

Mitty only claims to be a "trusted intermediary" ("TI") that acts solely as a conduit (see Mitty Col 1 line 9). A TI can take many forms. See: http://my.voyager.net/~lar/trusted_process.html and http://dbpubs.stanford.edu:8090/pub/1996-57 which describe a TI. Clearly a TI is not a CA.

PoS-e is a CA (See PoS-e at Abstract, and ¶¶ 0020, 0028, 0055, 0123, 0138, 0144, 0145, and Claims 1, 2, 12, 16, 17, 18, 19 and 22-through-82.

Mitty does not store "archives" other than as explained in Item 1.a., above. Mitty does not even refer to an "electronic package". The term "Electronic Package" in this context is created by PoS-e. Mitty only stores bits and pieces of a waybill (See Mitty Col. 7, lines 66-67 & Col 8, lines 1-5) which states:

> The logic proceeds to step **210** in which an electronic waybill data structure is created and initialized. An exemplary waybill structure includes a local date/time stamp including a time zone, the subject text, the filenames of any attachments, the e-mail address and DC

of sender **105,** addresses and certificates for the recipient(s) **120,** an account code, and client's billing code. The logic proceeds to step **215** in which....

In Mitty if the recipient's public key is not known, or if the recipient does not possess a public key, no transaction using the Mitty process is possible (See Mitty Col 8 line 4). In PoS-e only the recipient's email address is required because PoS-e is a CA and issues its own, proprietary, certificate and only PoS-e has the key which is referred to as an *In Camera Key* (ICK) which is completely private (See PoS-e ¶0028). Only PoS-e's CA (See PoS-e at ¶ 0020) has control of the ICK.

Thus, Mitty uses public keys any one can obtain which renders impossible for Mitty to ever be a CA. PoS-e creates its own ICK – which is totally private and confidential and accessible only by PoS-e's CA function – which fulfills all requirements of being a CA.

The only "particulars" stored by Mitty are fully discussed, above, under Item 1.a. Those particulars do not include (a) the actual files being transferred as attachment(s), (b) an exact and complete copy of the EP and (c) the ICK embedded in PoS-e's Electronic Certificate (See PoS-e at ¶ 0022). Therefore Mitty cannot re-create the ***exact*** EP that was transmitted. PoS-e specifically provides for such re-creation.

RESPONSE TO 1.c.: Mitty is not a CA (See Item 1.a and 1.b, above). Mitty does not deliver an EP the exact contents of which it can certify as being true and correct (See Mitty Col 7, lines 51 to Col 12, line 31). This is because Mitty is not a CA.

PoS-e is a CA and delivers an EP the exact contents of which PoS-e can certify as being true and correct (See PoS-e ¶¶ 0118 through 0170). This is because PoS-e is a CA.

RESPONSE TO 1.d.: The only "particulars" stored by Mitty are fully discussed, above, under Item 1.a. Those particulars do not include (a) the actual files being transferred as attachment(s), (b) an exact and complete copy of the EP and (c) the ICK embedded in PoS-e's Electronic Certificate (See PoS-e at ¶ 0022). Therefore Mitty cannot re-create the ***exact*** EP that was transmitted. PoS-e specifically provides for such re-creation.

Mitty is not a CA (See Item 1.a and 1.b, above). Mitty does not deliver an EP the exact contents of which it can certify as being true and correct (See Mitty Col 7, lines 51 to Col 12, line 31). This is because Mitty is not a CA. PoS-e is a CA and delivers an EP the exact contents of which PoS-e can certify as being true and correct (See PoS-e ¶¶ 0118 through 0170).

Mitty at Col 4 lines 30-60 only describes the "encrypted hash value" process applicable to all private key/public key encryption processes. Mitty **does not** create its own "encrypted hash value"! Mitty creates only (a) CRC[7] checks, and (b) electronic notaries[8] from sources unrelated to Mitty[9].

While Mitty creates an encrypted outer envelope (Mitty Col 2, lines 35-36) it creates no hash available to the sender or recipient of its own whatsoever. This is an additional reason why Mitty cannot be a CA.

Mitty details its ability to prove delivery at Col 15 lines 32-67. At Col 15 lines 47-55 the incredible weakness of the Mitty system is illustrated. This weakness makes Mitty wholly unsuitable to recreate a transaction even if Mitty were somehow construed as a CA (which it most certainly is not) because Mitty must go through the following steps:

---

[7] Cyclic Redundancy Check. A CRC is a type of check value designed to catch most transmission errors. A decoder calculates the CRC for the received data and compares it to the CRC that the encoder calculated, which is appended to the data. A mismatch indicates that the data was corrupted in transit. www.w3.org/TR/PNG-Glossary.html

[8] See Mitty Col 14, lines 49-57 which states:

> Under an exemplary embodiment, electronic notarization is performed as follows. The SDM1, IEM6, and RDMI are obtained from the database **117.** A digest, referred to as a notary hash, is then created of the combination SDMI+ IEM6+RDM1 wherein '+' indicates concatenation. The notary hash is then sent to an electronic notary service, e.g., Surety Corporation Notary Services available on the Internet, and the resulting notary seal as well as the notary hash are archived.

[9] Also, see Mitty Col 15, lines 3-5, which (as in footnote 5, above) clearly states the only hash mentioned in Mitty belongs to unrelated, third-party, universally-available internet electronic notaries.

- Checking that the VR sender's ID is registered with the system as active;
- Checking that the VR sender's account number is active;
- Checking that the VR number is registered;
- Checking that a CA can be found that is active and associated with the VR sender; and
- If only one of these checks proves negative, Mitty must then inform the sender indicating that Mitty has failed in its stated purpose of verifying transmission.

All DCs issued by trusted CAs are time-limited[10], thus if a Verification Request (VR) by a Mitty user is made after the expiration of a DC, there will be no way for Mitty to verify a transaction. As the issuance of DCs is driven by the ever-decreasing-cost economics model, people are constantly changing their CA and many people change their names, as well. Thus, Mitty won't work in this large number of cases!

[10] "To further reduce the possibility that someone will derive a private key from its public key, the certifying authority timestamps the key pair so that they must be replaced periodically, and provides an additional mechanism to assure that a signature was applied before the certificate expired." *What Are Digital Certificates?* By Microsoft (http://msdn.microsoft.com/library/default.asp?url=/library/enus/odeopg/html/deovrwhataredigitalcertificates.asp).

When trying to prove the DC of a recipient the same fault is found! If the recipient has changed CAs or her name, or the CA has gone out of business, proof of who the recipient is becomes impossible to obtain.

RESPONSE TO 1.e.: Mitty does not transmit a digital certificate, it is capable solely of addressing public keys available to anyone on the internet (See responses to Items 1.a. through 1.d., above).

The examiner indicates that Mitty transmits "an electronic certificate (digital certificate...)" citing Col 4, Lines 60-67. That reference in Mitty is only to the functions of companies that the Mitty process relies upon such as Thawte or Verisign, both of which are CAs.

Mitty simply "puts together" the public keys from different CAs which might not trust each other.

While anyone may sign public key records and act as an introducer in PGP, the PKIX framework requires that everyone will obtain certificates from a certification authority (CA). Relying parties who share a common CA can trust each other directly. Certificates from different CAs can't trust each other unless there is pre-trust relationship between the CAs.

RESPONSE TO 2-7: Mitty at Col 2, Lines 30-55 recites a system wherein the third-party encryption routines are utilized to secure a transmission underway; however, nothing there reveals what was is in the body of the transmission. What if a recipient's PKCS7 key is expired? Then Mitty cannot send the email.

Nothing in the Mitty patent discloses that it stores the entire EP, only bits and pieces of it.

RESPONSE TO 8; Mitty always sends the entire package according to Col 11, Lines 25-45. In the ordinary course of business it can be expected the message and attachments are quite large and, therefore, not able to be accepted by the recipient's email system. This creates a highly unstable transmission environment for the sender, including apprehension that an important EP will never be able to be delivered through a Mitty system.

PoS-e, on the other hand, retains the EP on its server, waiting for the recipient to log in and download the EP directly onto the recipients system, or to elect to maintain the EP on PoS-e's secure server, without resort to the highly undependable email system advocated by Mitty. See PoS-e at ¶ 0163. This creates a highly dependable and secure option for the recipient and much greater reliability than Mitty.

RESPONSE TO 9 and 10: Although Mitty discloses providing such information to the sender, that information is flawed in the typical embodiment of Mitty because of the probability of a high failure-to-deliver rate in cases of large attachments as argued above in Item I.8.

Even in cases where the embodiment mentioned briefly in Mitty at Col 13, Lines 60-68 through Col 14, Lines 1-5 is utilized, Mitty does not provide for the distribution to all senders, recipients and copy-to's (See PoS-e at ¶ 0080 and feature 110) of a CA signed Proof of Service and, therefore, PoS-e has invented a new principle of operation.

RESPONSE TO 11: It is believed that Mitty at Col 9, Lines 10-67 is a misunderstood reference because that reference does not teach what the Examiner relies upon it to be supposedly teaching.

In all of the 57 lines referenced the only mention of anything close to a "electronic certificate of service as an encrypted file" is found at Col 9, Lines 47-49 which teaches:

> Step 270 performs maintenance functions such as notifying the user that the document was sent and providing the waybill ID to the user.

Mitty teaches that the concept of the waybill ID is:

> The logic proceeds to step **245** in which a unique waybill ID is constructed and included in the waybill structure. To create the ID, a CRC value is generated of the encrypted message M3 and a digest of the encrypted message is generated. Date information is then concatenated with a digest of a string consisting of the CRC and the digest value of the encrypted message. (Mitty Col 8, Line 58-64)

Thus, the "waybill ID' of Mitty is but a random hash value of the underlying transaction's details, forever kept secret except to the user (See Mitty Col 9, Line 49).

PoS-e, on the other hand, teaches a whole new process and principle of operation, blazing a trail towards transparent disclosure that permits all interested persons to utilize PoS-e's Figure 12 for the public good, unlike Mitty which keeps its processes secret and clandestine.

Accordingly, PoS-e completely solves an entirely different problem from that proposed to be solved by Mitty and which Mitty only partially solves.

RESPONSE TO 12-18: Mitty at Col 4, Lines 30-67 and Col 5, Lines 1-26, is a misunderstood reference by the Examiner. Those sections teach only what is the state of the art for all digital signatures, not what is done by Mitty.

Enclosed Form 1449:

Enclosed is a Form 1449 disclosing, among other items, the PCT reasoned opinion that all of the Claims made by PoS-e therein were accepted. The PCT accepted said claims after Applicant provided the following argument of Applicant against the cited prior art of Feldbau number 6,182,219.

Prior Art: Feldbau

Unlike Feldbau, PoS-e has never been intended for use solely in the realm

However, Feldbau's limited scope and content do not teach any of the following, all of which are uniquely found in PoS-e:

1. That the certificate is printable but not modifiable;

2. That the certificate is automatically delivered to the sender, the recipient and all "copy-to's" (in fact, the copy-to concept is unique with PoS-e).

3. That the certificate on its face provides for a methodology of reconstructing the entirety of the transaction.

4. That the certificate on its face provides for a set term of years during which the certifying authority will reconstruct the entirety of the transaction.

In fact, Feldbau teaches (as discussed below) that it is not necessary to supply vital information about the sender, thus rendering the "certificate" of Feldbau legally incompetent and incomplete.

Feldbau exhibits a system that includes among its permutations paper technology (as evidenced by its xerographic copy system) up to electronic technology (embracing the internet and email), but all of its permutations are

sorely missing a single, crucial element: there is no system that is both legally competent and informationally complete that allows reconstruction of a transaction. PoS-e clearly fills that gaping lapse with its certificate that is both legally competent as a "proof of service" and factually complete, as well as being printable but not modifiable.

PoS-e's "Proof of Service – electronic", as discussed below, is legally competent. It has been accepted as proof of electronic delivery in federal court cases.[11] That acceptance was based upon the fact that all of the traditional elements of a proof of service are found in PoS-e and, additionally, the certifying authority is able with absolute certainty to reconstruct the transaction through PoS-e's use of the *in camera* key.

Feldbau, because its certificate is not protected from subsequent modifications by an outside party, because its certificate is able to be decrypted by any person employing Feldbau's public key, and because its certificate is not legally competent as a proof of service, is inherently untrustworthy and not admissible as evidence to prove anything.

[11] In fact, PoS-e certificates have been successfully utilized as "Proof of Service" in the following federal district court cases: Wynn Resorts Holdings, LLC, a Nevada limited liability company v. Iereve.com (PoS-e Internal Number 101975); MGM Mirage, a corporation v. MGM Gaming Systems (PoS-e Internal Number 102026).

Feldbau teaches that making a xerographic copy of a document – even though doing so voids the confidentiality of the original, and the process of making such a copy is highly error prone (especially when the copying is done by a disinterested clerk).

But, nowhere in Feldbau was the vital step taken between the objective – proving up a transmission on a commonsense basis – and the process. Feldbau possibly teaches a process; at least it was patented. But Feldbau reaches no workaday objective because, among other things, its certificate serves no independent purpose, its certificate is incompetent, its certificate is subject to corruption, and its system does not function to preserve the privacy of the electronic documents and computer files that are transferred through it.

A system operated according to new Claims 23-46, however, gives comfort to its users because of their knowledge that – no matter what happens to their own servers, local area networks, hard drives, or storage media – for those important and vital documents, the delivery of which may need to be proven-up at some time in the future for either a legal or mercantile purpose, PoS-e will be there to do it for them as an independent certifying authority for the period of years agreed upon (maximum at present is ten years).

The PoS-e system has since its inception protected the rights of the Sender. For example, see http://www.pos-e.com/htmls/proof.htm wherein it is clearly stated:

> "At any time subsequent to the delivery of a PoS-e-Gram, including a message and/or an attachment (sometimes herein referred to as an "electronic package"), any person who was a Sender, a Recipient, or a Copy-To (a person designated to receive a copy of the Certificate) may request that PoS-e deliver to them an electronic copy of what was sent. PoS-e will not provide a copy of any such electronic package to any other person without (a) the written consent of the Sender, or (b) a lawful court order."

Acceptance even in the file transfer industry itself has also occurred. For example, United Parcel Service (UPS) – a company that invested a reported $50 million in its electronic document transfer system – closed its doors after not being able to manage the business. Now, personnel from UPS use PoS-e to deliver their company's own, sensitive documentation.

PoS-e has attained additional acceptance in the legal community, as well, by now counting among its affiliates several bar associations that are entitled to share gross revenue generated by their members.

There is no known manifestation of the Feldbau invention. Arguably this may be because by its own limitations the "certificate" that is produced by its system is legally inadequate to serve any purpose, even as a certificate of a transaction – let alone as a proof of service. As stated herein, the Feldbau patent reveals that its authors consciously elected to limit the contents of its electronic certificate in such a manner as to render it useless in the business and legal worlds. Additionally, the certificate of Feldbau is nowhere indicated to be immutable. PoS-e's electronic proof of service, based on PDF, is not able to be modified in any way. Further:

A. Feldbau envisions a system whereby privacy of no document or electronic file is able to be maintained.

1. Feldbau's system allows for a clerk to copy a confidential document by a copy machine, for example (column 5, lines 15-30). In addition to the possibility of errors by way of missed pages, etc., all privacy is lost.

2. Feldbau' system additionally provides for public key encryption and states, "While the authentication methods described hereinabove refer mostly to symmetric digital signatures, a preferred authentication method may be obtained using public-key digital signatures. A major advantage of public-key digital

signatures over symmetric digital signatures is that they enable any third party (such as a judge), to verify the authenticity of both the data and the signer (where by using symmetric digital signatures, on a designated authenticator such as a secure device or a trusted third party, which have knowledge of the function, secret keys/codes etc., can perform the verification)." (Feldbau Col. 14, lines 58-67 and Col. 15, line 1)

3. A chief, and integral, feature of PoS-e is that it provides a system whereby the electronic package that was sent is able to be exactly reproduced.

4. In no case does Feldbau provide for absolute authentication that is a principal feature of PoS-e. This fact is exemplified by the collection and preservation by Feldbau of only "authentication information" (Feldbau inter alia column 3, lines 29-36). Further, the only information that is secured or stored in a secure location or device is the "authentication information" (Feldbau Col 4, Lines 37-39 and Col 9, lines 36-38).

5. PoS-e's *in camera* key is totally private and operated solely by the Certifying Authority (¶ 0028). Thus, every electronic package's contents are maintained as secrets.

6. Feldbau commercially envisions, and describes the use of a public key that is widely distributed and easily accessible, thus allowing anyone to discover the contents of any file.

a. For example, it is suggested that any person would be able to decrypt a file (Feldbau Cp; 14, line 63)

b. While the use of a private key is generally discussed, its actual use is not a functioning part of the patent.

7. Feldbau does not require the authentication of a Recipient's identity, as does PoS-e (see, for example PoS-e Figure 10) instead relying on "Received" or "Transmission OK" messages generated solely by a transceiver's protocol.

8. PoS-e's system requires that the Recipient identify herself upon entry into the secure server, which entry can only be done using a unique hash (PoS-e Figure 9) delivered to her by email (PoS-e Figure 4, item 157). Further, the Recipient is required to select a receipt method (by java applet, direct download, via email, or in another delivery method) (PoS-e Figure 11), all of which is logged (PoS-e at Figure 5, item 166).

9. Feldbau attempts unsuccessfully to grapple with its failure to ensure provable delivery by suggesting that the parties agree to use its system, and at (Feldbau Col 17, lines 55-58) wherein it is stated, "Alternatively, it may be agreed that multiple (two, three or more times of) certified dispatches of the message to be considered an acceptable proof of delivery and so forth." The whole point of "agreement" is superfluous because in the real world of serving documents, rarely (if ever) is there an agreement between parties to a law suit that an email may constitute proper service.

10. Combing the two-fold weakness of utilizing an unverifiable transceiver protocol along with insufficient transmission information renders the Feldbau system uncommercial.

11. PoS-e, on the other hand, is fully commercialized (see www.pos-e.com), has paying customers and a sound protocol designed to actually physically identify the receiver, exactly what the receiver received, and when.

12. PoS-e clearly seeks to keep the electronic package private (PoS-e at Figure 4A, item 154 f.).

13. Feldbau does not appear to show that the certifying authority encrypts the electronic package itself for the purpose of keeping it private

between the sender and recipient, and in doing so the certifying authority cannot guarantee 100% what was received as well as being able to reproduce the electronic package in the future.

14. PoS-e delivers to both the sender and recipient a complete copy of the electronic package, including any email message and all attachments, and makes it available to the sender for a term of years agreed upon by the sender.

15. PoS-e makes an exact copy available to the sender or recipient at any time under its defined "Future Query" process (¶¶ 0142 to 0146).

16. Making exact copies available to the sender and recipient during the agreed-upon subscription period (up to ten years) is a principal aspect of the current invention. The "crux" of this aspect of the PoS-e invention is that the sender and recipient always have an exact duplicate of the electronic package literally at their beck and call during the subscription period (¶ 0049).

17. Feldbau cannot serve this function because, as said on Feldbau (at Col 16, lines 19-25), "The service then provides back to the sender 701 a service's generated certificate 740 comprising the service's signature 742 and optionally various dispatch information elements from which it has been generated (there is no need to provide the message 702 and address 704 since they are already with the sender 701), thus the certificate 740 is typically tiny."

18. Additionally, Feldbau cannot provide under the breadth of his patent the inclusion in the said certificate of any information other than "...dispatch information elements" (Feldbau at Col lines 20-21).

B. In an innocent world, not providing a readily-available copy of the electronic package to the sender, and not including comprehensive details of the entire electronic package in the Feldbau certificate might work. But, that is not the world we live in. For example:

1. The PoS-e certificate is a "stand-alone" proof of service able to be entered as such[12] in any court of law because it fulfills all of the legal requirements of a "proof of service"; clearly, Feldbau's certificate could not, and does not!

2. Additionally, not providing a display of the complete core of an important transmission, such as is disclosed herein by PoS-e, defies common sense because the "message" and where it came from are of vital significance in proving delivery to a court. Aside from failing the best evidence rule, Feldbau's system cannot positively prove that (a) in the physical manifestation, its copy

[12] In fact, PoS-e certificates have been successfully utilized as "Proof of Service" in the following federal district court cases: Wynn Resorts Holdings, LLC, a Nevada limited liability company v. lereve.com (PoS-e Internal Number 101975); MGM Mirage, a corporation v. MGM Gaming Systems (PoS-e Internal Number 102026).

machine didn't miss a page, or two (or more) or that one page is printed partially (or, wholly) on top of another page, or that (b) in its electronic manifestation, the signed (See Feldbau, Figure 7, items 701 through 799) certificate relates in any way to the electronic package.

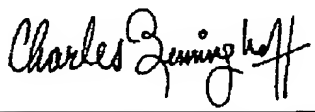
Response to Claim Rejections under U.S.C. §103

In lieu of the amendments to the claims made as a response as stated above, Applicant believes the Examiner misread the Mitty, Wong and Baker patents as relevant prior art against PoS-e.

Applicant would, therefore, ask the claims be allowed in light of the above responses to the §102(b) rejection.

Conclusion: We respectfully request the rejection of the claims be withdrawn in light of the amendments made to the claims and the Remarks made herein. Please allow claims 1-22 in the above-referenced application and allow it to proceed to issuance.

Respectfully submitted:



Charles Benninghoff, Applicant Pro Se

32071 Peppertree Bend
San Juan Capistrano, CA 92675

Appendix to Reply

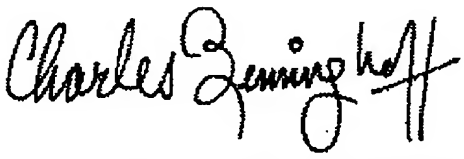
Commissioner for Patents

Washington DC 20231

Dear Commissioner:

Pursuant to Rule 121 the following is a true copy of the PCT International Preliminary Examination Report issued on 2 July 2003 but which the attorney working for the Applicant did not forward to you upon acceptance by the PCT.

Respectfully submitted:



Charles Benninghoff, Applicant Pro Se